paloalto NETWORKS | STRATA BY PALO ALTO NETWORKS

Three Use Cases for Securing a Hybrid Data Center

This paper provides network teams and their leadership insights into data center transformation and securing hybrid data centers while dramatically reducing security complexity.

Introduction

Network and IT leaders face a daunting challenge. IT is evolving into a business enabler by delivering services more quickly and closer to customers. Application workloads need to be able to move, based on business requirements, across on-premises data centers and multi-cloud deployments anywhere around the globe. These highly distributed application workloads move across the network at an unprecedented rate while dynamically growing and shrinking to address the on-demand deployment of applications.

To support this level of application elasticity and mobility, technologies such as virtualization, cloud, and software-defined networking are helping enterprises evolve their data centers to a hybrid model.

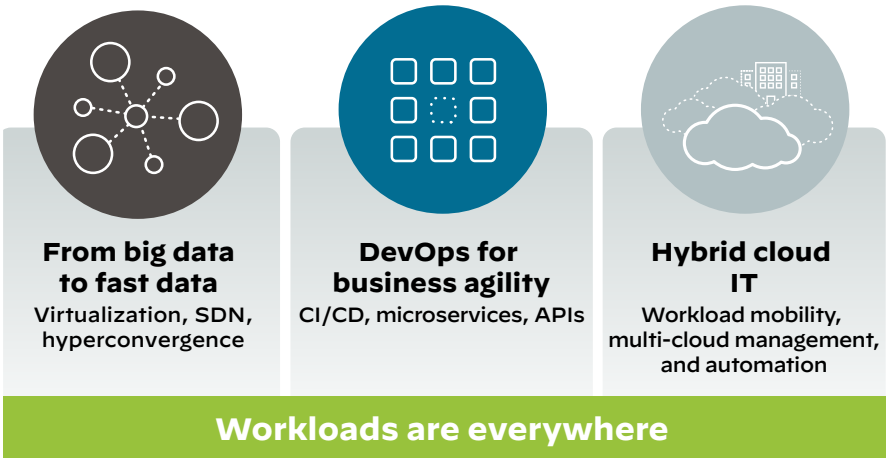

Figure 1: Dynamic changes in the data center

A modern, hybrid data center enables greater IT efficiency, automation, and agility, supporting the delivery of new application workloads across dynamic network fabric and hypervisor/virtual machine infrastructure. However, securing the hybrid data center requires a uniform security approach across physical, virtualized, and cloud environments while providing the best visibility, control, and next-generation threat protection.

Data Centers Are Fundamentally Changing

New Data Center Technologies

Big data analytics and new applications are bringing an explosion of data. To enable this transformation, enterprises are adopting technologies, including virtualization, software-defined networking (SDN), and hyperconverged infrastructure, that allow for the extension of new workloads into hybrid and multi-cloud deployments.

The elastic nature of workloads requires the network to scale up and out on demand, but this makes it difficult for data center teams to enforce security as the workloads move across data centers and clouds. Data center teams can't see where the workloads are, who is using them, or where those users are connecting from. The teams are also challenged to enforce proper access controls and implement a Zero Trust architecture. Fundamentally, security must be consistently enforced regardless of workload dynamics.

Changes in Application Development

Changes in DevOps and adoption of continuous integration/continuous deployment (CI/CD) pipelines are enabling business agility and growth. Software release pushes have moved from once or twice a year to many times per day. New application technologies, such as containers, microservices, and APIs, are changing the way applications are designed and deployed. Moreover, these new applications no longer reside in a single data center. Instead, they have components that run on-premises, in the cloud, across hybrid clouds, and even on end users' browsers. This new application development approach places great pressure on network teams to ensure

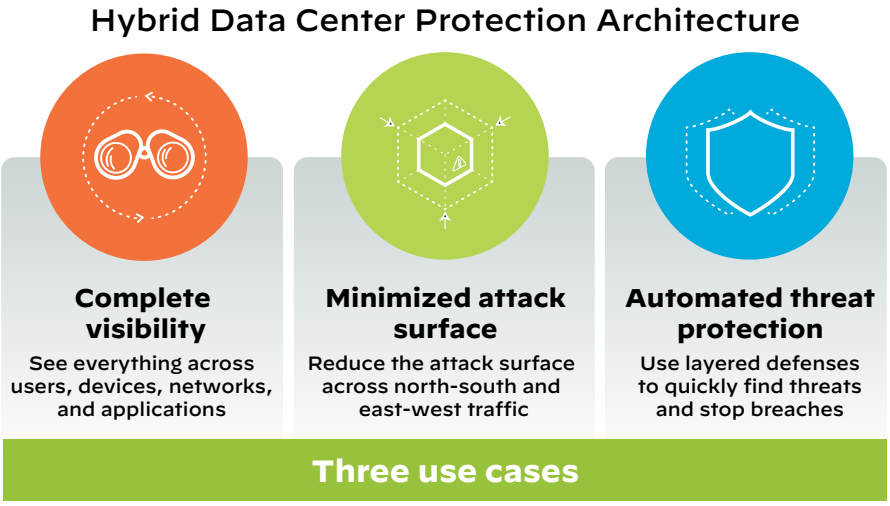

Figure 2: What's needed for hybrid data center security

their networks are robust, matching the agility and speed of DevOps as well as the line of business.

Orchestration of Workloads That Are Everywhere

As organizations race to the cloud to gain an economic advantage, data centers and clouds are often indistinguishable. Workloads can be orchestrated and provisioned across the cloud, and applications can reside on-premises one day and in the cloud the next day. This "lift and shift" practice is an underlying driver of the hybrid data center architecture. New orchestration tools allow workloads to be easily provisioned, deployed, and administered across multiple data center and cloud environments.

Network operations for the hybrid data center require full, continuous network insight to better manage security across the hybrid data center footprint as well as support orchestration of workloads across multiple locations and in a multi-cloud infrastructure.

Data center network teams protecting hybrid data centers with traditional security approaches face a security complexity trifecta: limited visibility and imprecise control, an ever-expanding attack surface, and increasingly advanced cyberthreats. Overcoming these requires adopting a new hybrid data center protection methodology to gain complete visibility, minimize the attack surface, and automate threat protection.

Three Use Cases to Protect the Hybrid Data Center

1. Gain Complete Visibility

Complete visibility—of who the users are, what applications they're accessing, and when and where they're connecting—is one of the biggest challenges for data center teams. Achieving this gives teams a comprehensive view of devices and connections so they can track applications and users. Application and user insights simplify network security management functions, such as installation, deployment, and maintenance, from a single console across all locations. This level of visibility also allows for the automation of effective Zero Trust policy implementation and deployment.

Palo Alto Networks Panorama™ network security management provides application and user insight while facilitating automation of effective security policy creation, implementation, and deployment. With greater visibility into the data center, network security teams can understand who is accessing what, when, and where, both inside the data center and across multi-cloud environments.

2. Minimize the Attack Surface

The best way to protect against advanced attacks, such as advanced persistent threats (APTs) or ransomware, is to minimize opportunities for attack and prevent the lateral movement of any threat in the data center. Multilayered segmentation enforces granular access control across north-south (using physical firewalls at the perimeter) and east-west traffic (via micro-segmentation using physical or virtual firewalls).

Palo Alto Networks physical and virtual Next-Generation Firewalls enable you to segment east-west traffic flows via microsegmentation and are easily integrated into the network fabric (e.g., on Cisco ACI® or Nexus® 9000 Series, or third-party switches such as Arista CloudVision®). In addition, our VM-Series Virtual Next-Generation Firewalls can be integrated at the hypervisor level to help secure virtualized infrastructure (e.g., across multiple hypervisors and SDN environments, such as VMware NSX®, Nutanix®). The VM-Series can help protect the perimeter and segment east-west traffic within multiple public clouds, such as Google Cloud Platform (GCP®), Amazon Web Services (AWS®), Microsoft Azure®, Alibaba Cloud, and Oracle Cloud®.

3. Automate Threat Protection

Palo Alto Networks multilayered defense enables you to discover threats and malicious activity, block threats in real time, and automatically isolate infected hosts to minimize business disruption as well as prevent data loss. This automated threat protection strategy for the hybrid data center requires broad coverage with tight integration, including the following functions:

- Threat prevention to block known threats and vulnerability attacks (network and application).
- Advanced malware analysis to automatically identify and protect against zero-day exploits.
- Security analytics to analyze endpoint and cloud telemetry for automatic detection and response to stealthy threats and insider attacks based on malicious network or host activity.
- Endpoint security to protect servers (physical or virtual, on-premises or cloud) from malware, exploits, and ransomware.

Dynamic Workload Security Made Simple with Palo Alto Networks

Data centers are evolving, with dynamic workloads that are everywhere. The days of considering the cloud and the data center distinct entities are over.

Working with Palo Alto Networks will enable you to transform your data center with confidence and help your business move faster. With our approach, you can significantly reduce complexity and develop a secure, hybrid data center architecture to deliver robust protection for your data and application workloads, everywhere.

Visit us online to learn more about how you can support business agility by safeguarding your data center.

paloalto NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com

3-use-cases-for-securing-a-hybrid-data-center-strata-b-100720